v8.2.0 Release Notes for X-Series Appliances

60221 | Release Notes | X-Series Appliances | 29-April-2016

Use these Release Notes to learn about what's new and improved for Forcepoint™ X-Series™ appliances in version 8.2.0.

Contents

If you are installing X-Series for the first time, be aware that X10G blade servers are delivered pre-loaded with the latest version of the product you ordered. They are ready for provisioning with the **firstboot** script. The Quick Start poster, Getting Started guide, and Switch Configuration guide are your comprehensive resources for installing the physical unit, running **firstboot**, and completing initial configuration.

If you are upgrading an existing deployment, you can upgrade directly from any version of 8.0.x using the express upgrade package. If you are upgrading from any version of 7.8.x, there is a quick three-step procedure. See the X-Series upgrade instructions for details.

See these companion Release Notes for information about the TRITON®security solutions that run on X-Series appliances:

- v8.2.0 Release Notes for Websense Web Protection Solutions
- v8.2.0 Release Notes for TRITON AP-EMAIL

See also:

- TRITON Manager Release Notes

And these supporting X-Series documents:

- Quick Start poster
- X10G Switch Configuration guide
- Using the X-Series Command Line Interface (CLI)

New in X-Series v8.2.0

60222 | Release Notes | X-Series Appliances | 29-April-2016

Introducing Forcepoint™

In January, 2016, Raytheon | Websense became Forcepoint LLC.

In this release all TRITON graphical user interfaces have a new look and feel. The colors and logos, as well as the logon screen and most toolbars, have been updated to reflect the Forcepoint brand.

These changes do not affect product functionality.

Over time, branding will be extended to other areas, such as the Help system, as well as to external content, such as the Knowledge Base.

Upgrade to 8.2.0 from 8.x and 7.8.x

Existing deployments can easily upgrade from any version of 8.1.x, 8.0.x, and 7.8.x. Follow the procedures described in the X-Series upgrade instructions. The procedure includes preparing and using a local filestore. This is a more efficient process because the upgrade patch files are downloaded from the Forcepoint patch file download server only once.

Express upgrade served from a local filestore

In version 8.0.0, a simpler, more efficient upgrade method, called **express upgrade**, was introduced. With express upgrade, when the CLI **load patch** command is run, in addition to listing all of the available individual module patches, the process inventories modules and versions on the appliance and offers an express upgrade option in which **load patch** both downloads all of the patches needed to upgrade to the latest version, and installs those patches in the correct order, thereby upgrading the appliance to the latest version in a single step.

Beginning with version 8.1.0, you can prepare a local filestore to offer the express upgrade option. This can be a big help because there are often many blades to upgrade and the time needed to download patches from a local filestore is usually much less than downloading them from the Websense patch file server. The Appliance controller module (APP) must be at version 8.1.0 to use this feature.

To support express upgrade from a local filestore, all of the individual patches that may be needed to upgrade a blade to the latest version must be placed in the filestore. Without these, **load patch** may not offer an express upgrade package that upgrades all of the appliance modules. Follow the detailed procedure described in the X-Series upgrade guide.

TRITON APX

Those upgrading from v7.8.4 and earlier need to know that version 8.0 introduced a new, simplified product naming and grouping of the TRITON product line.

Former Name	New Name
TRITON Web Security Gateway	TRITON AP-WEB
TRITON Web Security Gateway Anywhere	TRITON AP-WEB with: ◆ Web Hybrid Module ◆ Web DLP Module ◆ Web Sandbox Module
TRITON Email Security Gateway	TRITON AP-EMAIL
TRITON Email Security Gateway Anywhere	TRITON AP-EMAIL with: ◆ Email Hybrid Module

Existing product functionality is unchanged.

Appliance product names are unchanged.

Browsers supported with TRITON management consoles

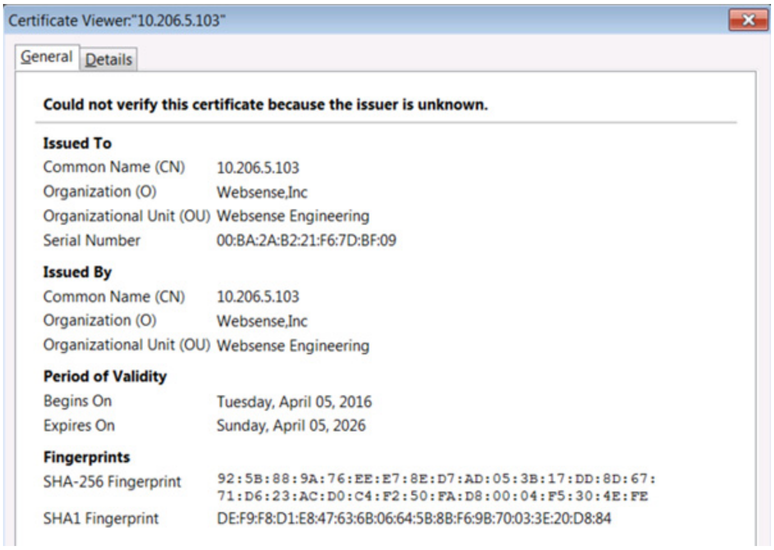
All deployments include a TRITON Manager. TRITON AP-WEB deployments include the Content Gateway manager. These managers can be used with the following browsers.

- Microsoft Internet Explorer 9 (non-compatibility mode)
- Microsoft Internet Explorer 10 – 11 (standard mode)
- Microsoft Edge 15, 20, and 25
- Mozilla Firefox versions 4.4 – 44
- Google Chrome 13 – 49

TRITON self-signed certificate

When you connect to any TRITON management console—TRITON Manager, and Content Gateway Manager—you are presented with a self-signed digital certificate. The certificate names Websense, Inc., as the Organization (O). This will change to Forcepoint LLC in a future release.

Because browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch a TRITON management console from a new browser. To avoid seeing this error, install or permanently accept the certificate in the browser. After the security certificate is accepted, the manager logon page is displayed.



Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	10.206.5.103
Organization (O)	Websense,Inc
Organizational Unit (OU)	Websense Engineering
Serial Number	00:BA:2A:B2:21:F6:7D:BF:09

Issued By

Common Name (CN)	10.206.5.103
Organization (O)	Websense,Inc
Organizational Unit (OU)	Websense Engineering

Period of Validity

Begins On	Tuesday, April 05, 2016
Expires On	Sunday, April 05, 2026

Fingerprints

SHA-256 Fingerprint	92:5B:88:9A:76:EE:E7:8E:D7:AD:05:3B:17:DD:8D:67: 71:D6:23:AC:D0:C4:F2:50:FA:D8:00:04:F5:30:4E:FE
SHA1 Fingerprint	DE:F9:F8:D1:E8:47:63:6B:06:64:5B:8B:F6:9B:70:03:3E:20:D8:84

Security enhancements

This release addresses the following Common Vulnerabilities and Exposures:

- **OpenSSL**

  OpenSSL libraries were updated to resolve the following vulnerabilities:

  CVE-2015-1788

  CVE-2015-1789

  CVE-2015-1790

  CVE-2015-1791

  CVE-2015-1792

  CVE-2014-8176

- **OpenLDAP**

  OpenLDAP libraries were updated to resolve the following vulnerability:

CVE-2013-4449
CVE-2012-3411

- **PAM** (Pluggable Authentication Modules)

  PAM libraries were updated to resolve the following vulnerabilities:

  CVE-2011-3148
  CVE-2011-3149

- **libgcrypt**

  libgcrypt libraries were updated to resolve the following vulnerability:

  CVE-2013-4242

- **util-linux-ng**

  util-linux-ng libraries were updated to resolve the following vulnerability:

  CVE-2013-0157

- **glibc**

  glibc libraries were updated to resolve the following vulnerability:

  CVE-2015-7547

- **libxml2**

  libxml2 libraries were updated to resolve the following vulnerability:

  CVE-2013-0338

Resolved and known issues

60223 | Release Notes | X-Series Appliances | 29-April-2016

A list of known issues in this release is available to customers who are registered at My Account.

If you are not currently logged in to My Account, the above link takes you to a login prompt. Log in to view the list.